

ORIGINAL

1 MICHAEL M. CARLSON (Bar No. 88048)
2 BRYAN J. WILSON (Bar No. 138842)
3 JANA G. GOLD (Bar No. 154246)
Morrison & Foerster
3 755 Page Mill Road
Palo Alto, California 94304-1018
4 Telephone: (415) 813-5600
Facsimile: (415) 494-0792

5 PATRICK J. FLINN (Bar No. 104423)
6 ALSTON & BIRD
One Atlantic Center
7 1201 West Peachtree Street
Atlanta, Georgia 30309
8 Telephone: (404) 881-7000
Facsimile: (404) 881-8777
9
10 Attorneys for Proposed Intervenor
CARO-KANN CORPORATION

FILED *mwa*

Nov 1 3 31 PM '95

RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA. S.J.

98

11
12
13 UNITED STATES DISTRICT COURT
14 NORTHERN DISTRICT OF CALIFORNIA
15
16 ROGER SCHLAFLY,
17 Plaintiff,
18 v.
19 PUBLIC KEY PARTNERS and
RSA DATA SECURITY, INC.,
20 Defendants.

No. CV 94 20512 SW

REPLY DECLARATION OF
JANA GOLD IN SUPPORT OF CKC'S
MOTION TO INTERVENE PURSUANT
TO FRCP 24(a)

Date: November 15, 1995
Time: 10:00 a.m.
Courtroom: 14

22
23
24 I, Jana Gold, declare:
25 1. I am an attorney with the law firm of Morrison & Foerster, attorneys of record for
26 proposed intervenor Caro-Kann Corporation. I make this declaration based on personal knowledge,
27 unless otherwise stated, and if called as a witness I could and would testify competently thereto.

28 GOLD REPLY DECL. IN SUPPORT
OF MOTION TO INTERVENE
CV 94 20512 SW

1 2. Attached to this declaration as Exhibit 1 is a true and correct copy of a document
2 clarifying the assignment of rights to sue on the Stanford patents as between Cylink Corporation and
3 Caro-Kann Corporation ("CKC").

4 3. Attached to this declaration as Exhibit 2 is a true and correct copy of PKP's responses
5 to Plaintiff's Requests for Admission in this case, served on October 23, 1995. Counsel for CKC did
6 not participate in drafting these responses and did not have an opportunity to review them before they
7 were served. I have been informed that CKC's president Robert Fougner did not participate in
8 drafting PKP's responses either.

9 4. Attached to this declaration as Exhibit 3 is a true and correct copy of a document
10 entitled "Information on Cylink's License Package" which was printed out by this office from
11 RSADSI's Home Page on the World Wide Web.

12 5. CKC moved to intervene in this case as soon as possible after the arbitrator's decision
13 was released, and noticed the motion for the first available date under the applicable rules of
14 procedure. When Mr. Schlaflay informed CKC of a scheduling conflict on that date, CKC agreed to
15 move the hearing to an earlier date, but explained to Mr. Schlaflay that it could not agree to reschedule
16 the motion for a later date because CKC did not want to delay upcoming dates for summary judgment
17 motions and other pre-trial and trial related dates.

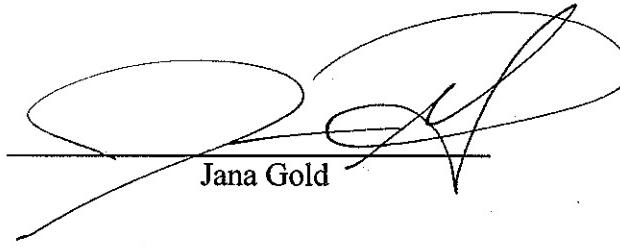
18 6. CKC does not intend to take any discovery in this action beyond the discovery that has
19 already been initiated by the current parties. CKC's counsel represented the inventors of the Stanford
20 patents in recent depositions taken by Mr. Schlaflay. CKC does intend to participate in ongoing
21 discovery and any additional discovery that may be propounded by the current parties.

22 I declare under penalty of perjury under the laws of the State of California that the foregoing
23 is true and correct.

24 Executed this 1st day of November, 1995 in Palo Alto, California.

25
26
27

28 GOLD DECL. IN SUPPORT
 OF MOTION TO INTERVENE
 CV 94 20512 SW



Jana Gold

1

ASSIGNMENT OF RIGHTS

This Agreement is entered into as of September 6, 1995, (the "Effective Date") by and between Cylink Corporation, a California Corporation having its principal place of business at 910 Hermosa Court, Sunnyvale, CA 94086 ("Cylink") and its wholly owned subsidiary, Caro-Kann Corporation, a California corporation having its principal place of business at 910 Hermosa Court, Sunnyvale, CA 94086 ("CKC").

WHEREAS, on August 25, 1989, The Board of Trustees of the Leland Stanford Junior University ("Stanford") granted Cylink an exclusive license (the Stanford License"), including the rights to institute actions against third parties for infringement and grant sublicenses, to the following U.S. Patents and their foreign equivalents (collectively, the "Patents"):

Cryptographic Apparatus and Method
("Hellman-Diffie") No. 4,200,770

Public Key Cryptographic Apparatus
and Method ("Hellman-Merkle") No. 4,218,582

Exponential Cryptographic Apparatus
and Method ("Hellman-Pohlig") No. 4,424,414

WHEREAS, on April 6, 1990, Stanford and Cylink agreed to amend Cylink's license and transfer certain of Cylink's rights, including the right to institute actions for infringement and to grant sublicenses to the Patents, to Public Key Partners, a California general partnership ("PKP") between CKC and RSA Data Security, Inc.;

WHEREAS, on September 6, 1995, a panel of duly appointed arbitrators issued their Decision and Order dissolving PKP;

WHEREAS, pursuant to the terms of the Stanford License, as amended, CKC now holds exclusive sublicensing rights to the Patents;

WHEREAS, CKC is currently in the business of sublicensing the Patents and is actively promoting licensing of the Patents to third parties;

WHEREAS, as between CKC and Cylink, it is CKC which has the responsibility for resolving claims for infringement of the Patents by third parties;

Assignment of Rights
Concerning Infringement
of Stanford Patents
Cylink and CKC

AND WHEREAS, Cylink and CKC wish to eliminate any ambiguity, to the extent that any ambiguity may exist, that CKC has the right as well as the responsibility for pursuing claims for infringement of the Patents by third parties;

NOW THEREFORE, it is hereby agreed, as follows:

1. All right, title and interest of Cylink to claims against third parties for infringement of the Patents, including the right to institute and prosecute actions against any such third parties for infringement, are hereby transferred and assigned to CKC, to the extent such rights are not already assigned to CKC.
2. All other rights of Cylink under the Stanford License shall remain in full force and effect.

Cylink Corporation



Robert B. Fougner
Corporate Secretary

A handwritten signature in black ink, appearing to read "John Doe".

RECED SEP 7 1995

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Roger Schlaflly, Pro Se
PO Box 1680
Sequel, CA 95073
telephone: (408) 476-3550

CALENDARED

10/08

In the United States District Court
for the Northern District of California

ROGER SCHLAFLY, Plaintiff) Case C-94-20512 SW PVT
v.) First Plaintiff Request
PUBLIC KEY PARTNERS, and) for Admission of Facts
RSA DATA SECURITY INC., Defendants.) Sept. 5, 1995

First Plaintiff Request for Admission of Facts. Defendants PKP and
RSADSI are requested to respond pursuant to FRCP Rule 36.

FIRST PLAINTIFF REQ ADM FACTS

page 1

1 Please admit the following as facts. Refer to Amended Complaint and
2 the Plaintiff's Motion for Partial Summary Judgment for definitions.
3

4 1. Exhibits A to Z, AA to AH of the Amended Complaint are all
5 authentic.
6

7 2. Exhibits CA to CI of the Plaintiff's Motion for Partial Summary
8 Judgment are all authentic.
9

10 3. Each reference to "Diffie" in the above exhibits is to the same
11 person. Likewise with Rivest, Hellman, Merkle, Adleman, Shamir,
12 Bidzos, Fougner, Schlaflly, and Schnorr.
13

14 4. Each and every allegation in the Amended Complaint.
15

16 5. Exhibit CA is a copy of a document which was publicly distributed
17 in August 1976.
18

19 6. Exhibit CA is a full disclosure of the Diffie-Hellman invention.
20

21 7. Exhibit CA is a preprint of Exhibit U.
22

23 8. The Diffie-Hellman invention was disclosed to the public in a
24 lecture by Diffie in June 1976.
25

26 9. The Diffie-Hellman invention was disclosed to the public in a
27 lecture by Hellman in June 1976.
28

1 10. The fundamental ideas of public key cryptography are disclosed
2 in Exhibit T.

3
4 11. The Diffie-Hellman patent does not disclose or claim a public
5 key cryptosystem.

6
7 12. The account given in Exhibit V of the breaking of the trapdoor
8 knapsack is accurate.

9
10 13. The trapdoor knapsack described in Exhibit V is the same
11 invention as that disclosed in the Hellman-Merkle patent.

12
13 14. Merkle paid off bets of \$100 and \$1000 when the Hellman-Merkle
14 invention was shown to not meet its stated objectives.

15
16 15. The \$1000 offered in Exhibit CC was paid to Ernie Brickell in or
17 around 1985.

18
19 16. The Hellman-Merkle patent disclosure does not enable someone
20 skilled in the art (up to 1978) to make a secure cryptosystem.

21
22 17. As a matter of law, a Hellman-Merkle patent claim is invalid
23 unless it is realized by at least one of its disclosed embodiments.

24
25 18. The only two embodiments of a cryptosystem disclosed in Hellman-
26 Merkle are what is commonly called the "trapdoor knapsack" and the
27 "multiple iteration knapsack".

1 19. None of the embodiments disclosed in Hellman-Merkle achieve any
2 of the objects of the invention stated in col. 2 of the patent.

3
4 20. The methods of claims 4 and 5 of Hellman-Merkle are not shown in
5 any of the patent diagrams.

6
7 21. The method of claims 4 of Hellman-Merkle is a method for what is
8 commonly called "digital signature with message recovery".

9
10 22. No practical method for digital signatures is disclosed in
11 Hellman-Merkle.

12
13 23. The computational infeasibility of Hellman-Merkle patent claims
14 1-6 and 14-17 is not achieved by any of the disclosed embodiments,
15 where "computationally infeasible" is defined as in Exhibit T or
16 as in col. 5, lines 10-14, of the Hellman-Merkle patent.

17
18 24. There is a consensus in the cryptographic community that the
19 Hellman-Merkle invention is useless.

20
21 25. The Hellman-Merkle invention is useless.

22
23 26. PKP partners RSADSI and Cylink have known the Hellman-Merkle
24 invention to be worthless since at least 1985, and have not used it
25 in their commercial products.

26
27 27. The Hellman-Merkle invention is fully disclosed in Exhibit CE.

1 28. Exhibit CB is an accurate account of the failure of the Hellman-
2 Merkle invention.

3
4 29. The Hellman-Merkle patent does not disclose a method of digital
5 signature generation or verification which avoids message encryption.

6
7 30. Practice of the DSA does not infringe the Schnorr patent.

8
9 31. The "rejuvenation" scheme of Schnorr, specified in col. 9-10 and
10 claim 5 of the Schnorr patent, has been broken and does not achieve
11 the claimed security. In particular, it does not achieve the object
12 of the invention stated in col. 2, line 25-30.

13
14 32. Claim 5 of the Schnorr patent is invalid and unenforceable.

15
16 33. Exhibit CD is a full disclosure of the RSA invention.

17
18 34. The practice of the RSA invention is enabled by Exhibit U,
19 section V of Exhibit CD, and standard computer science textbooks
20 available in 1977.

21
22 35. The RSA invention is fully disclosed in Exhibit CE.

23
24 36. The RSA invention is fully disclosed in Exhibit CF.

25
26 37. The RSA invention is fully disclosed in Exhibit CI.

27
28 38. RSADSI regards any cryptographic applications of the formula

$$Y = X^e \text{ mod } N,$$

1 where N is a large composite number, to be an infringement of the
2 RSA patent.

3
4 39. There is a four-line Perl script which RSADSI regards as an
5 infringement of the RSA patent.

6
7 40. PKP never offered ISC a patent license.

8
9 41. PKP has never complied with the IEEE patent policy.

10
11 42. PKP led ANSI to believe it would comply with the ANSI patent
12 policy when ANSI drafted its X9.31 proposed standard for RSA
13 signatures.

14
15 43. PKP has refused to give ANSI the assurances necessary for ANSI
16 to adopt X9.31 as a standard.

17
18 44. The federal Digital Signature Standard was delayed at least a
19 year by PKP asserting patent claims against the DSA.

20
21 45. Fougner has asserted that the US Government may not practice the
22 DSA without obtaining a license to the Schnorr patent.

23
24 46. Bidzos has threatened lawsuits against users of the DSA who fail
25 to license PKP patents.

26
27 47. The best mode disclosed in the Diffie-Hellman patent is what is
28 popularly called the single iteration trapdoor knapsack.

1 48. The RSA patent does not disclose any novel hardware.
2

3 49. The RSA invention is fully disclosed in Exhibit CI.
4

5 50. A public key cryptosystem is not secure if it is feasible for an
6 adversary to compute the private key from the corresponding public
7 key.
8

9 Dated: Sept 5, 1995
10

11 By: Roger Schlafly
12

13 Plaintiff, Roger Schlafly, Pro Se
14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1 Thomas R. Hogan, Esq., California State Bar No. 042048
2 John P. Shinn, Esq., California State Bar No. 175598
3 LAW OFFICES OF THOMAS R. HOGAN
4 60 South Market Street, Suite 1123
5 San Jose, CA 95113-2332
Telephone: (408) 292-7600
6
7 Attorneys for Defendant
8 PUBLIC KEY PARTNERS
9
10

11 UNITED STATES DISTRICT COURT
12 FOR THE NORTHERN DISTRICT OF CALIFORNIA
13
14

15 ROGER SCHLAFLY,) No. CV 94 20512 SW (FVT)
16 Plaintiff,)
17 v.)
18 PUBLIC KEY PARTNERS and)
19 RSA DATA SECURITY, INC.,)
20 Defendants.)
21 _____
22
23

DEFENDANT PUBLIC KEY PARTNERS'
RESPONSES TO FIRST PLAINTIFF
REQUEST FOR ADMISSION OF FACTS

24 PROPOUNDING PARTY: Plaintiff, ROGER SCHLAFLY
25 RESPONDING PARTY: Defendant, PUBLIC KEY PARTNERS
26 SET NUMBER: One
27 Pursuant to Federal Rule of Civil Procedure, defendant PUBLIC
28 KEY PARTNERS, does hereby respond to the Request for Admissions
served by plaintiff, above-named, as follows:
29
30

REQUEST FOR ADMISSION NO. 1

Exhibits A to Z, AA to AH of the Amended Complaint are all
authentic.

31 ////
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
181

1 RESPONSE TO REQUEST FOR ADMISSION NO. 1

2 Objection: PKP objects to this request on the grounds that
3 it is vague, ambiguous and unintelligible in that PKP has to
4 speculate as to the meaning of the word "authentic" as used in
5 this request.

6 Defendant Public Key Partners cannot truthfully admit or deny
7 this allegation for the reason that although defendants have made
8 reasonable inquiry, defendants have been unable to locate the
9 source of or verify the authenticity of said documents and,
10 therefore, the information known to them is insufficient to admit
11 or deny the same.

12 REQUEST FOR ADMISSION NO. 2

13 Exhibits CA to CI of the Plaintiff's Motion for Partial
14 Summary Judgment are all authentic.

15 RESPONSE TO REQUEST FOR ADMISSION NO. 2

16 Objection: PKP objects to this request on the grounds that
17 it is vague, ambiguous and unintelligible in that PKP has to
18 speculate as to the meaning of the word "authentic" as used in
19 this request.

20 Defendant Public Key Partners cannot truthfully admit or deny
21 this allegation for the reason that although defendants have made
22 reasonable inquiry, defendants have been unable to locate the
23 source of or verify the authenticity of said documents and,
24 therefore, the information known to them is insufficient to admit
25 or deny the same.

26 / / / /

27 / / / /

28 / / / /

1 REQUEST FOR ADMISSION NO. 3

2 Each reference to "Diffie" in the above exhibits is to the
3 same person. Likewise with Rivest, Hellman, Merkle, Adleman,
4 Shamir, Bidzos, Fougner, Schlaflly, and Schnorr.

5 RESPONSE TO REQUEST NO. 3

6 Defendant Public Key Partners cannot truthfully admit or deny
7 this allegation for the reason that although defendants have made
8 reasonable inquiry, defendants have been unable to locate the
9 source of or verify the accuracy of said documents and, therefore,
10 the information known to them is insufficient to admit or deny the
11 same.

12 REQUEST FOR ADMISSION NO. 4

13 Each and every allegation in the Amended Complaint.

14 RESPONSE TO REQUEST FOR ADMISSION NO. 4

15 PKP incorporates herein by reference each and every
16 admission, denial and denial on information and belief that it
17 stated in its Answer to the Amended Complaint.

18 REQUEST FOR ADMISSION NO. 5

19 Exhibit CA is a copy of a document which was publicly
20 distributed in August 1976.

21 RESPONSE TO REQUEST FOR ADMISSION NO. 5

22 PKP lacks sufficient information and belief with which to
23 admit or deny this Request, and, on that basis, denies this
24 Request.

25 REQUEST FOR ADMISSION NO. 6

26 Exhibit CA is a full disclosure of the Diffie-Hellman
27 invention.

28 RESPONSE TO REQUEST FOR ADMISSION NO. 6

1 PKP lacks sufficient information and belief with which to
2 admit or deny this Request, and, on that basis, denies this
3 Request.

4 REQUEST FOR ADMISSION NO. 7

5 Exhibit CA is a preprint of Exhibit U.

6 RESPONSE TO REQUEST FOR ADMISSION NO. 7

7 PKP cannot truthfully admit or deny this allegation for the
8 reason that although defendants have made reasonable inquiry,
9 defendants have been unable to locate the source of or verify the
10 accuracy of said documents and, therefore, the information known
11 to them is insufficient to admit or deny the same.

12 REQUEST FOR ADMISSION NO. 8

13 The Diffie-Hellman invention was disclosed to the public in a
14 lecture by Diffie in June 1976.

15 RESPONSE TO REQUEST FOR ADMISSION NO. 8

16 PKP lacks sufficient information and belief with which to
17 admit or deny this Request, and, on that basis, denies this
18 Request.

19 REQUEST FOR ADMISSION NO. 9

20 The Diffie-Hellman invention was disclosed to the public in a
21 lecture by Hellman in June 1976.

22 RESPONSE TO REQUEST FOR ADMISSION NO. 9

23 PKP lacks sufficient information and belief with which to
24 admit or deny this Request, and, on that basis, denies this
25 Request.

26 REQUEST FOR ADMISSION NO. 10

27 The fundamental ideas of public key cryptography are
28 disclosed in Exhibit T.

1 RESPONSE TO REQUEST FOR ADMISSION NO. 10

2 Objection: PKP objects to this request on the grounds that
3 it is vague, ambiguous and unintelligible in that PKP has to
4 speculate as to the meaning of the word "fundamental" as used in
5 this request. Without waiving this objection, PKP lacks
6 sufficient information and belief with which to admit or deny this
7 Request, and, on that basis, denies this Request.

8 REQUEST FOR ADMISSION NO. 11

9 The Diffie-Hellman patent does not disclose or claim a public
10 key cryptosystem.

11 RESPONSE TO REQUEST FOR ADMISSION NO. 11

12 PKP lacks sufficient information and belief with which to
13 admit or deny this Request, and, on that basis, denies this
14 Request.

15 REQUEST FOR ADMISSION NO. 12

16 The account given in Exhibit V of the breaking of the
17 trapdoor knapsack is accurate.

18 RESPONSE TO REQUEST FOR ADMISSION NO. 12

19 PKP lacks sufficient information and belief with which to
20 admit or deny this Request, and, on that basis, denies this
21 Request.

22 REQUEST FOR ADMISSION NO. 13

23 The trapdoor knapsack described in Exhibit V is the same
24 invention as that disclosed in the Hellman-Merkle patent.

25 RESPONSE TO REQUEST FOR ADMISSION NO. 13

26 PKP lacks sufficient information and belief with which to
27 admit or deny this Request, and, on that basis, denies this
28 Request.

1 REQUEST FOR ADMISSION NO. 14

2 Merkle paid off bets of \$100 and \$1000 when the Hellman-
3 Merkle invention was shown to not meet its stated objectives.

4 RESPONSE TO REQUEST FOR ADMISSION NO. 14

5 PKP lacks sufficient information and belief with which to
6 admit or deny this Request, and, on that basis, denies this
7 Request.

8 REQUEST FOR ADMISSION NO. 15

9 The \$1000 offered in Exhibit CC was paid to Ernie Brickell in
10 or around 1985.

11 RESPONSE TO REQUEST FOR ADMISSION NO. 15

12 PKP lacks sufficient information and belief with which to
13 admit or deny this Request, and, on that basis, denies this
14 Request.

15 REQUEST FOR ADMISSION NO. 16

16 The Hellman-Merkle patent disclosure does not enable someone
17 skilled in the art (up to 1978) to make a secure cryptosystem.

18 RESPONSE TO REQUEST FOR ADMISSION NO. 16

19 PKP lacks sufficient information and belief with which to
20 admit or deny this Request, and, on that basis, denies this
21 Request.

22 REQUEST FOR ADMISSION NO. 17

23 As a matter of law, a Hellman-Merkle patent claim is invalid
24 unless it is realized by at least one of its disclosed
25 embodiments.

26 RESPONSE TO REQUEST FOR ADMISSION NO. 17

27

28

1 PKP lacks sufficient information and belief with which to
2 admit or deny this Request, and, on that basis, denies this
3 Request.

4 REQUEST FOR ADMISSION NO. 18

5 The only two embodiments of a cryptosystem disclosed in
6 Hellman-Merkle are what is commonly called the "trapdoor knapsack"
7 and the "multiple iteration knapsack".

8 RESPONSE TO REQUEST FOR ADMISSION NO. 18

9 PKP lacks sufficient information and belief with which to
10 admit or deny this Request, and, on that basis, denies this
11 Request.

12 REQUEST FOR ADMISSION NO. 19

13 None of the embodiments disclosed in Hellman-Merkle achieve
14 any of the objects of the invention stated in col. 2 of the
15 patent.

16 RESPONSE TO REQUEST FOR ADMISSION NO. 19

17 PKP lacks sufficient information and belief with which to
18 admit or deny this Request, and, on that basis, denies this
19 Request.

20 REQUEST FOR ADMISSION NO. 20

21 The methods of claims 4 and 5 of Hellman-Merkle are not shown
22 in any of the patent diagrams.

23 RESPONSE TO REQUEST FOR ADMISSION NO. 20

24 PKP lacks sufficient information and belief with which to
25 admit or deny this Request, and, on that basis, denies this
26 Request.

27 REQUEST FOR ADMISSION NO. 21

28

1 The method of claims 4 of Hellman-Merkle is a method for what
2 is commonly called "digital signature with message recovery".

3 RESPONSE TO REQUEST FOR ADMISSION NO. 21

4 PKP lacks sufficient information and belief with which to
5 admit or deny this Request, and, on that basis, denies this
6 Request.

7 REQUEST FOR ADMISSION NO. 22

8 No practical method for digital signatures is disclosed in
9 Hellman-Merkle.

10 RESPONSE TO REQUEST FOR ADMISSION NO. 22

11 PKP lacks sufficient information and belief with which to
12 admit or deny this Request, and, on that basis, denies this
13 Request.

14 REQUEST FOR ADMISSION NO. 23

15 The computational infeasibility of Hellman-Merkle patent
16 claims 1-6 and 14-17 is not achieved by any of the disclosed
17 embodiments, where "computationally infeasible" is defined as in
18 Exhibit T or as in col. 5, lines 10-14, of the Hellman-Merkle
19 patent.

20 RESPONSE TO REQUEST FOR ADMISSION NO. 23

21 PKP lacks sufficient information and belief with which to
22 admit or deny this Request, and, on that basis, denies this
23 Request.

24 REQUEST FOR ADMISSION NO. 24

25 There is a consensus in the cryptographic community that the
26 Hellman-Merkle invention is useless.

27 RESPONSE TO REQUEST FOR ADMISSION NO. 24

28

1 PKP lacks sufficient information and belief with which to
2 admit or deny this Request, and, on that basis, denies this
3 Request.

4 REQUEST FOR ADMISSION NO. 25

5 The Hellman-Merkle invention is useless.

6 RESPONSE TO REQUEST FOR ADMISSION NO. 25

7 PKP lacks sufficient information and belief with which to
8 admit or deny this Request, and, on that basis, denies this
9 Request.

10 REQUEST FOR ADMISSION NO. 26

11 PKP partners RSADSI and Cylink have known the Hellman-Merkle
12 invention to be worthless since at least 1985, and have not used
13 it in their commercial products.

14 RESPONSE TO REQUEST FOR ADMISSION NO. 26

15 PKP objects to this Request on the ground that this Request
16 is properly directed to non-party Caro-Kann Corporation and/or
17 RSADSI, who has more information on which to base an admission or
18 denial to this request.

19 REQUEST FOR ADMISSION NO. 27

20 The Hellman-Merkle invention is fully disclosed in Exhibit
21 CE.

22 RESPONSE TO REQUEST FOR ADMISSION NO. 27

23 PKP lacks sufficient information and belief with which to
24 admit or deny this Request, and, on that basis, denies this
25 Request.

26 REQUEST FOR ADMISSION NO. 28

27 Exhibit CB is an accurate account of the failure of the
28 Hellman-Merkle invention.

1 RESPONSE TO REQUEST FOR ADMISSION NO. 28

2 PKP lacks sufficient information and belief with which to
3 admit or deny this Request, and, on that basis, denies this
4 Request.

5 REQUEST FOR ADMISSION NO. 29

6 The Hellman-Merkle patent does not disclose a method of
7 digital signature generation or verification which avoids message
8 encryption.

9 RESPONSE TO REQUEST FOR ADMISSION NO. 29

10 PKP lacks sufficient information and belief with which to
11 admit or deny this Request, and, on that basis, denies this
12 Request.

13 REQUEST FOR ADMISSION NO. 30

14 Practice of the DSA does not infringe the Schnorr patent.

15 RESPONSE TO REQUEST FOR ADMISSION NO. 30

16 PKP denies this Request.

17 REQUEST FOR ADMISSION NO. 31

18 The "rejuvenation" scheme Schnorr, specified in col. 9-10 and
19 claim 5 of the Schnorr patent, has been broken and does not
20 achieve the claimed security. In particular, it does not achieve
21 the object of the invention stated in col. 2, line 25-30.

22 RESPONSE TO REQUEST FOR ADMISSION NO. 31

23 PKP objects to this Request on the grounds that it is
24 irrelevant and not calculated to lead to the discovery of
25 admissible evidence. Without waiving this objection, PKP responds
26 that it lacks sufficient information and belief with which to
27 admit or deny this Request, and, on that basis, denies this
28 Request.

1 **REQUEST FOR ADMISSION NO. 32**

2 Claim 5 of the Schnorr patent is invalid and unenforceable.

3 **RESPONSE TO REQUEST FOR ADMISSION NO. 32**

4 PKP objects to this Request on the grounds that it is
5 irrelevant and not calculated to lead to the discovery of
6 admissible evidence. Without waiving this objection, PKP responds
7 that it lacks sufficient information and belief with which to
8 admit or deny this Request, and, on that basis, denies this
9 Request.

10 **REQUEST FOR ADMISSION NO. 33**

11 Exhibit CD is a full disclosure of the RSA invention.

12 **RESPONSE TO REQUEST FOR ADMISSION NO. 33**

13 PKP objects to this Request on the ground that this Request
14 is properly directed to defendant RSADSI, who has more information
15 on which to base an admission or denial to this request.

16 **REQUEST FOR ADMISSION NO. 34**

17 The practice of the RSA invention is enabled by Exhibit U,
18 section V of Exhibit CD, and standard computer science textbooks
19 available in 1977.

20 **RESPONSE TO REQUEST FOR ADMISSION NO. 34**

21 PKP objects to this Request on the ground that this Request
22 is properly directed to defendant RSADSI, who has more information
23 on which to base an admission or denial to this request.

24 **REQUEST FOR ADMISSION NO. 35**

25 The RSA invention is fully disclosed in Exhibit CE.

26 **RESPONSE TO REQUEST FOR ADMISSION NO. 35**

27

28

1 PKP objects to this Request on the ground that this Request
2 is properly directed to defendant RSADSI, who has more information
3 on which to base an admission or denial to this request.

4 REQUEST FOR ADMISSION NO. 36

5 The RSA invention is fully disclosed in Exhibit CF.

6 RESPONSE TO REQUEST FOR ADMISSION NO. 36

7 PKP objects to this Request on the ground that this Request
8 is properly directed to defendant RSADSI, who has more information
9 on which to base an admission or denial to this request.

10 REQUEST FOR ADMISSION NO. 37

11 The RSA invention is fully disclosed in Exhibit CI.

12 RESPONSE TO REQUEST FOR ADMISSION NO. 37

13 PKP objects to this Request on the ground that this Request
14 is properly directed to defendant RSADSI, who has more information
15 on which to base an admission or denial to this request.

16 REQUEST FOR ADMISSION NO. 38

17 RSADSI regards any cryptographic applications of the formula
18
$$Y = X^e \text{ mod } N,$$

19 where N is a large composite number, to be an infringement of the
20 RSA patent.

21 RESPONSE TO REQUEST FOR ADMISSION NO. 38

22 PKP objects to this Request on the ground that this Request
23 is properly directed to defendant RSADSI, who has more information
24 on which to base an admission or denial to this request.

25 REQUEST FOR ADMISSION NO. 39

26 There is a four-line Perl script which RSADSI regards as an
27 infringement of the RSA patent.

28 RESPONSE TO REQUEST FOR ADMISSION NO. 39

1 PKP objects to this Request on the ground that this Request
2 is properly directed to defendant RSA/DSI, who has more information
3 on which to base an admission or denial to this request.

4 REQUEST FOR ADMISSION NO. 40

5 PKP never offered ISC a patent license.

6 RESPONSE TO REQUEST FOR ADMISSION NO. 40

7 Denied.

8 REQUEST FOR ADMISSION NO. 41

9 PKP has never complied with the IEEE patent policy.

10 RESPONSE TO REQUEST FOR ADMISSION NO. 41

11 Denied.

12 REQUEST FOR ADMISSION NO. 42

13 PKP led ANSI to believe it would comply with the ANSI patent
14 policy when ANSI drafted its X9.31 proposed standard for RSA
15 signatures.

16 RESPONSE TO REQUEST FOR ADMISSION NO. 42

17 PKP denies any negative connotation associated with
18 plaintiff's use of the phrase "PKP led ANSI to believe." Except
19 as expressly denied, PKP admits this Request.

20 REQUEST FOR ADMISSION NO. 43

21 PKP has refused to give ANSI the assurances necessary for
22 ANSI to adopt X9.31 as a standard.

23 RESPONSE TO REQUEST FOR ADMISSION NO. 43

24 Denied.

25 REQUEST FOR ADMISSION NO. 44

26 The federal Digital Signature Standard was delayed at least a
27 year by PKP asserting patent claims against the DSA.

28 RESPONSE TO REQUEST FOR ADMISSION NO. 44

1 PKP lacks sufficient information and belief on which to admit
2 or deny this Request, and, on that basis, denies this Request.

3 REQUEST FOR ADMISSION NO. 45

4 Fougner has asserted that the US Government may not practice
5 the DSA without obtaining a license to the Schnorr patent.

6 RESPONSE TO REQUEST FOR ADMISSION NO. 45

7 PKP admits this Request.

8 REQUEST FOR ADMISSION NO. 46

9 Bidzos has threatened lawsuits against users of the DSA who
10 fail to license PKP patents.

11 RESPONSE TO REQUEST FOR ADMISSION NO. 46

12 PKP denies this Request.

13 REQUEST FOR ADMISSION NO. 47

14 The best mode disclosed in the Diffie-Hellman patent is what
15 is popularly called the single iteration trapdoor knapsack.

16 RESPONSE TO REQUEST FOR ADMISSION NO. 47

17 PKP responds that it lacks sufficient information and belief
18 with which to admit or deny this Request, and, on that basis,
19 denies this Request.

20 REQUEST FOR ADMISSION NO. 48

21 The RSA patent does not disclose any novel hardware.

22 RESPONSE TO REQUEST FOR ADMISSION NO. 48

23 PKP objects to this Request on the ground that this Request
24 is properly directed to defendant RSADSI, who has more information
25 on which to base an admission or denial to this request.

26 REQUEST FOR ADMISSION NO. 49

27 The RSA invention is fully disclosed in Exhibit CI.

28 RESPONSE TO REQUEST FOR ADMISSION NO. 49

1 PKP objects to this Request on the ground that this Request
2 is properly directed to defendant RSADSI, who has more information
3 on which to base an admission or denial to this request.

4 **REQUEST FOR ADMISSION NO. 50**

5 A public key cryptosystem is not secure if it is feasible for
6 an adversary to compute the private key from the corresponding
7 public key.

8 **RESPONSE TO REQUEST FOR ADMISSION NO. 50**

9 PKP admits this Request.

10
11 Dated: 10/23/95


12 THOMAS R. HOGAN
13 JOHN P. SHINN

14 Attorneys for Defendant
15 PUBLIC KEY PARTNERS

21
22
23
24
25
26
27
28

3



Information on Cylink's "License Package"

TO: All Current and Potential RSA Software Customers

RSA has been informed that some of our licensees have received a "license package" from Robert Fougner at Cylink, offering to license the so-called Stanford Patents, and threatening legal reprisals to those who do not. The package contains serious inaccuracies that are clearly self-serving and constructed to coerce the recipient into an unnecessary license.

We would advise everyone to remember to always take Cylink's statements with a rather large grain of salt. We realize that the Cylink package is frightening, and we are saddened to see that, in their frustration in their inability to successfully attack RSA, Cylink's venom for us has been directed against our customers.

RSA specific recommendation/policy respecting the Cylink package is as follows:

1. It is RSA's position that our licensees **do not need** a Stanford Patent license from Cylink in order to use the software licensed by RSA, as long as the RSA licensee complies with the terms of their RSA license.
2. The final decision to license the Stanford Patents is up to the individual RSA customer, though we strongly recommend that they not do so. Contrary to implications made by Cylink in their license package, RSA will not reimburse licensees for any sums paid to Cylink for a Stanford Patent license. We feel that Cylink is attempting to coerce our customers into buying an expensive license that is not necessary.
3. If Cylink ever backs up its threats and actually sues any RSA licensee based on infringement of the Stanford Patents, we will stand behind the indemnity provisions of our license agreements and vigorously defend our customers, at our expense.

In fact, we've already taken steps to protect our licensees by filing a lawsuit in Federal Court specifically seeking a declaration that a Stanford Patent license is not necessary for the use of RSA's software.

Our final word is this: RSA will continue to take whatever steps are necessary to protect our licensees.

If you have any questions or comments, please do not hesitate to contact Paul Livesay, RSA's Director of Legal Affairs, at 415/595-8782.

| [RSA Home](#) | [What's New](#) |

Copyright © 1995 RSA Data Security, Inc. All rights reserved.
10/17/95